

AN 1998-161979 JAPIO

TI USER AUTHENTICATION BY FINGERPRINT AT TIME OF LOG-IN TO SERVER AND

CONVERTED PASSWORD

IN ISONO TAKAO; KATO TOMOYA

PA HITACHI LTD

PI \*\*\*JP 10161979\*\*\* A 19980619 Heisei

AI JP 1996-315924 (JP08315924 Heisei) 19961127

PRAI JP 1996-315924 19961127

SO PATENT ABSTRACTS OF JAPAN (CD-ROM), Unexamined Applications, Vol. 1998

IC ICM G06F015-00

AB PROBLEM TO BE SOLVED: To prevent illegal log-in even when a user ID and a password are stolen in the case of user authentication by the user ID and the password at a system where a client utilizes a server.

SOLUTION: A fingerprint recognizing device 30 is added to a client 20, three input requests of user ID, password and fingerprint are outputted at the time of user log-in, when the fingerprint relevant to the user ID is inputted, the inputted password is converted and a certificate request is outputted to a server 10 by the inputted user ID and the converted password. At the client 20, the algorithm for converting the password is programmed. The user ID and the password to be converted on the side of client 20 are previously registered in the server 10. This password registered in the server 10 is made different from the password to be inputted by the user, and made secret. The user is certified by the inputted user ID and the secret password registered in the server 10.

COPYRIGHT: (C)1998,JPO

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-161979

(43)公開日 平成10年(1998)6月19日

(51)Int.Cl.\*

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

3 3 0 F

3 3 0 E

審査請求 未請求 請求項の数1 OL (全4頁)

(21)出願番号

特願平8-315924

(71)出願人

000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者

磯野 孝雄

神奈川県川崎市幸区鹿島田890番地の12

株式会社日立製作所情報システム事業部内

(72)発明者

加藤 友哉

愛知県名古屋市中区栄三丁目10番22号 日

立中部ソフトウェア株式会社内

(74)代理人

弁理士 小川 勝男

(22)出願日

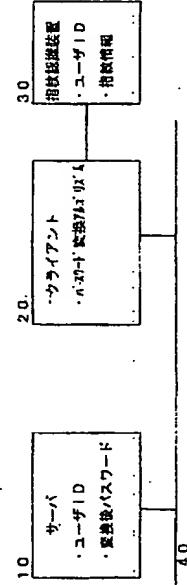
平成8年(1996)11月27日

(54)【発明の名称】 サーバへログイン時の指紋、及び変換したパスワードによるユーザ認証

(57)【要約】

【課題】サーバをクライアントが利用するシステムにおいて、ユーザIDとパスワードによるユーザ認証の際、ユーザIDとパスワードが盗まれた場合でも、不正ログインを防止できるようにする。

【解決手段】クライアントに指紋認識装置を付け、ユーザログイン時に、ユーザID、パスワード、指紋の3つの入力要求を出し、ユーザIDに該当する指紋が入力された場合、入力されたパスワードを変換し、入力されたユーザIDと変換されたパスワードでサーバへ認証要求を出す。クライアントではパスワードを変換するアルゴリズムを組み込んでおく。サーバにはあらかじめ、ユーザIDとクライアント側で変換されるパスワードを登録しておく。このサーバに登録されたパスワードは、ユーザが入力するものとは異なり、秘密にしておく。ユーザの認証は入力されたユーザIDとサーバに登録された秘密のパスワードで行う。



## 【特許請求の範囲】

【請求項1】クライアントからユーザがサーバへログインするシステムにおいて、クライアントに指紋認識装置を接続しておき、ログイン時に、ユーザIDとパスワードにより、ユーザ認証を行う際、クライアント側で、ユーザがユーザID、パスワード入力後に、指紋入力要求を出し、ユーザIDに該当する指紋が入力されたか判定し、ユーザIDに該当する指紋が入力された場合、パスワードにアルゴリズムで変換をかけ、入力されたユーザIDと変換したパスワードでサーバに対し認証要求を出し、サーバはユーザ認証を行い、認証の可否をクライアントに通知し、ログイン完了または、ログイン拒否とし、ユーザIDに該当しない指紋が入力された場合、ログイン拒否とするユーザ認証方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、コンピュータシステムにおいて、クライアントからサーバにログインする際のユーザ認証方法に関する。

## 【0002】

【従来の技術】サーバへユーザがログインする際、クライアントから入力された、ユーザIDとパスワードにより、サーバがユーザ認証を行う。指紋認証を個人識別に用いた技術は、その装置の使用可否の認証、例えばドアの開閉やパソコンの使用可否に利用されている。クライアントサーバシステムのユーザ認証に指紋認識を適用した場合、サーバ、クライアント両者に指紋によるユーザ認証の仕組みを作り込む必要がある。

【0003】本発明は、ユーザIDとパスワードによるユーザ認証と指紋によるユーザ認証を組み合わせ、クライアント側だけの変更で、より高度なセキュリティを実現するものである。

## 【0004】

【発明が解決しようとする課題】従来の、サーバへのログイン時にクライアントから入力されたユーザIDとパスワードによるユーザ認証では、入力時に盗み見みされて、ユーザIDとパスワードが盗まれ、不正ログインされる欠点があった。

【0005】本発明の目的は、ユーザIDとパスワードが盗まれた場合でも、不正ログインを防止することにある。

## 【0006】

【課題を解決するための手段】上記目的を解決するため、本発明ではクライアントに指紋認識装置を付け、ユーザログイン時に、ユーザID、パスワード、指紋の3つの入力要求を出し、ユーザIDに該当する指紋が入力された場合、入力されたパスワードを変換し、入力されたユーザIDと変換されたパスワードでサーバへ認証要求を出す。クライアントではパスワードを変換するアルゴリズムを組み込んでおく。サーバにはあらかじめ、ユ

ーザIDとクライアント側で変換されるパスワードを登録しておく。このサーバに登録されたパスワードは、ユーザが入力するものとは異なり、秘密にしておく。ユーザの認証は入力されたユーザIDとサーバに登録された秘密のパスワードで行う。

## 【0007】

【発明の実施の形態】本発明の一実施例について図面により詳細に説明する。

## 【0008】図1は本発明を適用したシステムの一実施

10 例のシステム構成図である。図1において、10はサーバ、20はクライアント、30は指紋認識装置、40はサーバ10とクライアント20を結ぶLAN等の通信回線である。本実施例ではクライアントは1台しか示されていないが、勿論、実際にはこれ以上のクライアントがサーバ10と結ばれていることは云うまでもない。

【0009】サーバ10には、ユーザIDとパスワードが登録しており、クライアント20から送信されるユーザIDとパスワードで認証され、クライアント20がサーバ10の機能を利用することができる。指紋認識装置

20 30はユーザIDと指紋データのデータベースを持ち、ユーザIDと指紋の照合を行い、クライアント20はパスワードを変換するアルゴリズムを有し、パスワード変換を行う。

【0010】次に、本ユーザ認証の方法を図2のフローチャートに従い説明する。図2は、クライアント20がサーバ10へログインが完了するまでの流れを示したものである。クライアント20がサーバ10へログインを行うために、ユーザIDとパスワードを入力する(ステップ100)。

30 【0011】クライアント20に指紋入力要求が表示され、ユーザは指紋認識装置に指紋を入力する(ステップ110)。指紋認識装置30はユーザIDと入力された指紋が正しいか照合を行い、結果をクライアント20へ通知する(ステップ120)。クライアント20は指紋認識装置30から通知された結果を判断し(ステップ130)、NGの場合、ユーザID、パスワード入力画面にエラー表示する。OKの場合、クライアント20は入力されたパスワードを変換アルゴリズムに従い変換する(ステップ140)。クライアント20は入力されたユーザIDと変換されたパスワードをサーバ10へ送信する(ステップ150)。サーバ10は受信したユーザIDとパスワードが、サーバ10に登録されているユーザIDとパスワードと等しいか照合する(ステップ160)。

40 照合結果を判断し(ステップ170)、結果がNGの場合クライアント20にエラー通知を行う。結果がOKの場合、ログイン完了をクライアント20へ通知する(ステップ180)。以上で、サーバ10とクライアント20のユーザ認証処理は完了し、クライアント20はサーバ10を利用することができる。

50 【0012】次に、ユーザIDとパスワードの関係を具

体例を用いて説明する。

【0013】例えば、サーバ10に登録されたユーザIDがuser1、パスワードが12345とした場合、クライアント20でユーザが入力するユーザIDはuser1、パスワードはABCDEとする。クライアント20のパスワード変換アルゴリズムはABCDEを12345に変換するものを作り込んでおく。この場合のユーザ認証の流れは、クライアント20にユーザID user1、パスワードABCDEが入力される。指紋認識装置30はユーザID user1に該当する指紋が入力されたか照合し、正しい場合クライアント20はパスワードABCDEを12345に変換し、サーバ10へ照合を依頼する。ここでユーザ認証の完了となる。

【0014】サーバにはユーザIDとパスワードによる認証しかなくても、クライアントに本発明を適用すれば、より高度なセキュリティを確保することが可能となる。

【0015】

【発明の効果】以上説明したように、既存のクライアントがサーバを利用する製品にこの方法を適用すれば、正規ユーザが本発明を適用したクライアントからユーザID、パスワードを入力するところを不正ユーザが盗み見し、指紋認識装置のないクライアント製品（既存の製品）を用意して、サーバへログインを試みても、サーバでは、パスワードが異なるため、ログインを拒否する。

【0016】このように、本発明の適用で、セキュリティを大幅に向かう。

【図面の簡単な説明】

10 【図1】本発明の一実施例を示すシステム構成図である。

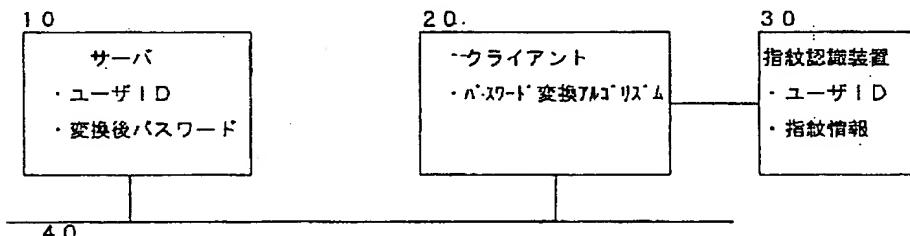
【図2】ユーザ認証の方法を示すフローチャートである。

【符号の説明】

- 10 サーバ
- 20 クライアント
- 30 指紋認識装置
- 40 通信回線。

【図1】

図1



[図2]

図2

サーバ10

クライアント20

指紋認機装置30

